## Risk register

### **Operational environment:**

The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premise employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts. The bank's services are marketed by a professional sports team and ten local businesses in the community. There are strict financial regulations that require the bank to secure their data and funds, like having enough cash available each day to meet Federal Reserve requirements.

| **Asset** | **Risk(s)** | **Description** | **Likelihood** | **Severity** | **Priority** |
| --- | --- | --- | --- | --- | --- |
| Funds | Business email compromise | *An employee is tricked into sharing confidential information.* | 1 | 2 | low |
| Compromised user database | *Customer data is poorly encrypted.* | 3 | 3 | high |
| Financial records leak | *A database server of backed up data is publicly accessible.* | 3 | 3 | high |
| Theft | *The bank's safe is left unlocked.* | 3 | 3 | high |
| Supply chain disruption | *Delivery delays due to natural disasters.* | 1 | 3 | moderate |
| Notes | *How are security events possible considering the risks the asset faces in its operating environment?*  *Security events are possible due to the vulnerabilities that are present in the bank systems. This vulnerability can be exploited by malicious threat actors. Thus, there are inherent risks in the systems. For example the customer data is poorly encrypted which means malicious actors could exploit it to breach the user database and steal valuable information which could lead to reputational damage, fines by regulatory authorities and financial loss to the bank. Another notable event is the leak in financial bank records due to the weakness of exposing the internal database to the public, this database server should have been labeled restricted and not open to the public.*  *The bank also risks theft by leaving the bank;s safe unlocked. This allows potential disgruntled employees to take advantage of the situation to steal funds. Thus it is important for the bank to have physical security in place to mitigate such risk* | | | | |

**Asset:** The asset at risk of being harmed, damaged, or stolen.

**Risk(s):** A potential risk to the organization's information systems and data.

**Description:** A vulnerability that might lead to a security incident.

**Likelihood:** Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.

**Severity:** Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.

**Priority:** How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

## Sample risk matrix





|  | Low  1 | Moderate  2 | Catastrophic  3 |
| --- | --- | --- | --- |
| Certain  3 | 3 | 6 | 9 |
| Likely  2 | 2 | 4 | 6 |
| Rare  1 | 1 | 2 | 3 |